UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- *v.* -	:	S1 19 Cr. 00794 (KPF)
TOMER OSOVITZKI, a/k/a "Tom Osovitzki,"	:	
Defendant.	:	

GOVERNMENT'S OMNIBUS MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT TOMER OSOVITZKI'S PRETRIAL MOTIONS

AUDREY STRAUSS
Acting United States Attorney for the
Southern District of New York
Attorney for the United States of America

Jeffrey C. Coffman
Micah F. Fergenson
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

I. OVERVIEW

The Government respectfully submits this memorandum in opposition to the 16 separate October 23, 2020 motions of defendant Tomer Osovitzki. Specifically, the defendant has filed the following pretrial motions or requests:

- Motion to Suppress Fruits of Search Warrant for Cellphone Location and Pen Register Information (Dkt. No. 48) ("Cellphone Location Motion")
- Motion to Suppress Fruits of Search Warrant Regarding Stored Electronic Communications (Dkt. No. 49) ("Email Motion")
- Motion to Suppress Fruits of Search Warrant Regarding Premises-1 (Dkt. No. 50) ("Office Motion")
- Motion to Suppress Fruits of Search Warrant Regarding Premises-2 (Dkt. No. 51) ("Home Motion")
- Motion to Suppress Fruits of Search Warrant Regarding Premises-3 (Dkt. No. 52) ("Parents' Residence Motion")
- Motion to Suppress Fruits of Search Warrant Regarding Premises-4 (Dkt. No. 53) ("Apartment Residence Motion")
- Motion to Suppress Fruits of Search Warrant Regarding the Defendant's Vehicle (Dkt. No. 54) ("Hummer Motion")
- Motion for Relief from Prejudicial Joinder of Charges (Dkt. No. 55)
- Motion to Disclose and Produce *Brady* (Exculpatory) Material (Dkt. No. 56)
- Motion for Disclosure Pursuant to Rules 404(b) and 609 (Dkt. No. 57)
- Motion for Disclosure of any and all Co-Conspirator Statements the Prosecution Intends to Introduce at Trial (Dkt. No. 58)
- Motion for Early Production of *Jencks* Material (Dkt. No. 59)
- Motion to Exclude Evidence of Offer or Settlement Pursuant to Rule 408 (Dkt. No. 60)
- Request for Notice of Intent to Call Expert Witnesses and Discovery Pursuant to Rule 16(a)(1)(F) and (G) (Dkt. No. 63)
- Request for Notice by Government of Intent to Introduce Evidence Pursuant to Rule 807 (Dkt. No. 64)

- Motion for Preservation of Recordings and Notes (Dkt. No. 65)

This memorandum consolidates the Government's opposition to the defendant's filings, organized as follows: (1) opposition to the defendant's search-warrant-related motions to suppress (Dkt. Nos. 48-54); (2) opposition to the defendant's motion to sever counts for trial (Dkt. No. 55); (3) opposition to the defendant's Rule 408 motion (Dkt. No. 60); and (4) opposition to the defendant's miscellaneous motions relating to notice, disclosure, and preservation (Dkt Nos. 56-59, 63-65).

These motions should all be denied. *First*, the defendant's motions to suppress are meritless because the search warrants: (a) were based upon probable cause supported by sworn affidavits, described with particularity the places to be searched and the things to be seized, and were not overbroad; (b) were, in any event, relied on in good faith; and (c) Osovitzki lacks standing to challenge the searches of certain email accounts and his parents' residence. *Second*, separate trials on each count in the Superseding Indictment are neither necessary nor warranted. *Third*, the defendant has not established that the evidence referenced in his Rule 408 motion actually implicates Rule 408, and to the extent that the Government develops an intention to introduce evidence that may implicate Rule 408, the Government plans to confer with the defense and if necessary brief the admissibility of that evidence *in limine*. *Fourth*, the defendant's miscellaneous motions for disclosure and preservation orders are unripe, non-specific, and/or moot.

II. BACKGROUND

On November 7, 2019, a grand jury sitting in this District returned Superseding Indictment S1 19 Cr. 794 (the "Indictment"), which charges Osovitzki with conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1349 and 1343 (Count One); wire fraud, in violation of 18 U.S.C. § 1343 (Count Two); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) (Count Three). As alleged therein, from in or about March 2017 through September 2018, Osovitzki, who

operated a private charter flight brokerage business, conspired to perpetrate a scheme to defraud American Express ("Amex"), credit card processors, aircraft charter companies, and other merchants by, among other things, inducing the aircraft charter companies and other merchants to process credit card transactions (1) under the false pretense that the transactions had been approved by Amex (the "Force-Post Transactions") and/or (2) with credit card account numbers belonging to other account holders, without those account holders' authorization (the "Unauthorized Card Transactions").

III. THE DEFENDANT'S MOTIONS TO SUPPRESS EVIDENCE SEIZED PURSUANT TO THE SEARCH WARRANTS SHOULD BE DENIED

The defendant contends that the seven search warrants in this case were issued without probable cause, lacked particularity, and were overbroad. The defendant's motions should be denied in their entirety. As each of the three reviewing United States Magistrate Judges properly concluded, the search warrant applications articulated probable cause to believe that evidence of specific crimes would be found in the locations that were the subjects of the warrants, and each warrant clearly and specifically described the items to be seized. Moreover, even assuming a subsequent court were to disagree with one of the approving judges' determinations, the defendant identifies no basis for concluding that the law enforcement agents acted in anything short of good faith reliance in executing those warrants. *See generally United States v. Leon*, 468 U.S. 897 (1984). In addition, Osovitzki lacks standing to challenge the searches of his parents' residence and three of the six email accounts at issue.

A. Background

On December 20, 2018, Magistrate Judge Debra Freeman approved, based on the facts set forth in a sworn affidavit, a search warrant directing Microsoft to produce all content and other information associated with six email accounts utilized in connection with the defendant's charter

flight brokerage businesses (the "Email Warrant" and "Email Affidavit"). (Dkt. No. 49, Ex. 1). On April 10, 2019, Magistrate Judge Sarah Netburn approved, based on the facts set forth in a sworn affidavit, a search warrant directing Verizon Wireless to produce prospective location information for one of Osovitzki's cellphones. (Dkt. No. 48, Ex. 1 (the "Cellphone Location Warrant" and "Cellphone Location Affidavit")). On May 22, 2019, Magistrate Judge Lisette M. Reid approved, based on the facts set forth in sworn affidavits, search warrants for the following:

- Osovitzki's business office (Dkt. No. 50, Ex. 1 (the "Office Warrant" and "Office Affidavit"));
- The home of Osovitzki and his wife (Dkt. No. 51, Ex. 1 (the "Home Warrant" and "Home Affidavit"));
- Osovitzki's parents' residence (Dkt. No. 52, Ex. 1) (the "Parents' Residence Warrant" and "Parents' Residence Affidavit"); and
- A luxury apartment Osovitzki had recently rented and at which he was then residing (Dkt. No. 53, Ex. 1 (the "Apartment Residence Warrant" and "Apartment Residence Affidavit")).

Finally, on May 23, 2019, Judge Reid approved, based on the facts set forth in a sworn affidavit, a search warrant for Osovitzki's Hummer sport utility vehicle. (Dkt. No. 54, Ex. 1 (the "Hummer Warrant" and "Hummer Affidavit")). As noted, in support of these warrants, the lead Federal Bureau of Investigation ("FBI") agent involved in the investigation submitted detailed sworn affidavits (collectively, the "Supporting Affidavits").

1. The Supporting Affidavits' Probable Cause to Believe That the Defendant and Jetlux Committed the Subject Offenses

The Supporting Affidavits each identified Subject Offenses[1] and set forth substantially the same basic facts to establish probable cause that Osovitzki and his company, Jetlux, Inc.

[1] *See* Email Aff. ¶ 4 (wire fraud and conspiracy to commit the same); Cellphone Location Aff. ¶ 7 (wire fraud); Office Aff. ¶ 4 (wire fraud and aggravated identity theft); Home Aff. ¶ 4 (wire fraud and aggravated identity theft); Parents' Residence Aff. ¶ 4 (wire fraud and aggravated

("Jetlux")—which was a Florida corporation that brokered airline and private charter flights (*see, e.g.*, Email Aff. ¶¶ 9-10)—had engaged in the credit card scheme. Those facts included the following:

a. The "Force-Post" Transactions

- Credit card point of sale devices ("POSDs") may be used by merchants to "force-post" credit card transactions in order to override a declined transaction at a POSD, using legitimate authorization codes obtained from the financial institutions that issue credit cards. A "force-post" transaction may be used to override a declined transaction even when a credit card account does not have sufficient available credit, when a credit card account has been cancelled by the financial institution that issued the card, or when a credit card account number that has never even been issued by the financial institution. Unfortunately, many merchants are not aware of this potential misuse of authorization codes, and assume that if a "force-post" transaction is completed through a POSD, then the code was legitimate, when in fact only authorization codes provided by the financial institutions that issue credit cards are valid as confirmation that the transactions have been approved by the financial institution, and a merchant who uses an authorization code that was not in fact provided by the financial institution bears the risk of not receiving payment for the transaction. (*E.g.*, Email Aff. ¶¶ 11(a)-(c)).

- Osovitzki, his wife, and his mother, previously held Amex credit cards, but Amex had cancelled these cards by August 2017, January 2018, and November 2017, respectively (*E.g.* Email Aff. ¶¶ 11(d)-(f)).[2]

- From in or about March 2017, through at least in or about March 2018, Osovitzki and agents of Jetlux repeatedly presented these credit card account numbers as payment for charter flights and other goods and services. The transactions were or would have been declined by Amex had they been processed normally through a POSD, because the cards had been cancelled by Amex or because the accounts did not have sufficient available credit. Osovitzki and agents of Jetlux provided fraudulent authorization codes to those victim merchants, duping them into processing "force-post" transactions. Osovitzki falsely told merchants, including through email correspondence, that he had obtained the authorization codes from Amex. (*E.g.*, Email Aff. ¶ 12).

- Based upon Osovitzki and Jetlux's false representations, merchants conducted "force-post" transactions, using the Osovitzki Credit Cards and authorization codes that had not in fact

identity theft); Apartment Residence Aff. ¶ 4 (wire fraud and aggravated identity theft); Hummer Aff. ¶ 4 (wire fraud and aggravated identity theft).

[2] All but the initial affidavit also included information about force-post transactions on a second Amex card held by Osovitzki's mother, which Amex deactivated in or about November 2018. (*E.g.* Cellphone Location Aff. ¶ 10(h)).

by provided by Amex. (*Id.*). These transactions were later declined by Amex, resulting in a total loss in excess of $2 million to victim merchants, and included the following:

- Approximately 30 instances, from March 2017 through March 2018, in which Osovitzki's Amex credit card was used by approximately 13 victim merchants to process "force-post" transactions in a total amount of approximately $1,156,944, the vast majority occurring after Osovitzki's Amex card had been cancelled. (*E.g.*, Email Aff. ¶¶ 11(d), 12(a)-(c)).

- Approximately eight instances, from September 2017 through February 2018, in which Osovitzki's wife's Amex credit card was used, by approximately eight victim merchants, to process "force-post" transactions in a total amount of approximately $973,561. (*E.g.*, Email Aff. ¶ 12(d)).

- Two instances in January and February 2018, in which one of Osovitzki's mother's Amex credit cards[3] was used to process "force-post" transactions totaling more than $185,000 for charter flights, after Osovitzki emailed invalid authorization codes to the charter flight company ("Victim-3"), and falsely stated, among other things, that Amex had provided those authorization codes. (*E.g.*, Email Aff. ¶¶ 12(e)-(g)).

- On or about February 5, 2018, a victim ("Victim-3") informed Osovitzki by email that Victim-3 had been informed that morning by its credit card vendor that the transactions it had processed to Osovitzki's mother's Amex credit card were fraudulent or otherwise being disputed. Osovitzki responded, by email: "I think [Osovitzki's mother's first name] got confused here She saw 2 charges and got confused and scared," and instructed Victim-3 to process the $156,723 in two transactions (in the amounts of approximately $75,000 and $81,733) on Osovitzki's cancelled Amex credit card. Later that day, Osovitzki sent Victim-3 an email stating that he had "obtained the authorization" and provided Victim-3 with two purported authorization codes. Again, Amex had actually provided neither of these authorization codes. However, as instructed, Victim-3 "force-posted" the transactions, which were later declined by Amex. (*E.g.*, Email Aff. ¶¶ 12(h)-(i)).

- After Victim-3 provided the charter flights referenced in the foregoing paragraph, and Amex informed Victim-3 that it was declining the approximately $262,075 of "force-posted" transactions Victim-3 had processed with Osovitzki's Amex credit card at Osovitzki's direction, Osovitzki told Victim-3 that: (i) he was unwilling to send payment until Amex reversed the charges to his card; (ii) he would make payment by wire; (iii) he needed Amex to "return the money;" (iv) he would being sending Victim-3 small partial payments while he waited for his "overpayment check;" and (v) Jetlux had experienced "internal theft and we have had to take a loan to pay this." Although Osovitzki and Victim-

[3] All but the initial Email Affidavit also detailed approximately 24 "force-post" transactions conducted with Osovitzki's mother's second Amex card, in a total amount of approximately $369,640, from on or about December 30, 2018 through on or about March 1, 2019. (*E.g.* Cellphone Location Aff. ¶ 22).

3 agreed upon a payment plan in March 2018, Jetlux did not make the required payments under the plan. (*E.g.*, Email Aff. ¶ 12(j)).

b. The Unauthorized Credit Card Transactions

- A company that used Jetlux as a broker to purchase charter flights ("Customer-1") provided Jetlux with its Amex credit card account number in connection with those business dealings. From on or about April 6, 2017, through on or about October 26, 2017, Jetlux provided Customer-1's Amex account number to approximately 11 charter flight companies for charter flights that Customer-1 did not request, authorize, or utilize, resulting in unauthorized transactions in a total amount of approximately $668,000. (*E.g.*, Email Aff. ¶¶ 13(a)-(c)).

- Another company that used Jetlux as a broker to purchase charter flights ("Customer-2") provided Jetlux with its Amex Account number in connection with those business dealings. From on or about September 6, 2017, through October 3, 2017, Jetlux provided Customer-2's Amex account number to approximately 13 charter flight companies for charter flights that Customer-2 did not request, authorized, or utilize, including at least one flight for which Osovitzki was listed as a passenger. Several of the charter companies informed Customer-2 that a Jetlux employee had booked the trips. Customer-2 informed Amex that it had not authorized Jetlux to use the its Amex account in connection with the approximately 18 separate credit card transactions associated with these flights, which were in a total amount of approximately $531,000. (*E.g.*, Email Aff. ¶¶ 13(d)-(e)).

- In or about April 2018, Jetlux booked an April 2, 2018 flight with an Austria-based charter flight company ("Charter Company-1"), for a charter flight from Shanghai to Paris for a celebrity ("Celebrity-2") and her associates, at a price of approximately $126,000. Jetlux failed to make payment for the flight by wire to Charter Company-1 prior to the flight's departure. When Charter Company-1 demanded payment before the flight would depart, on or about April 2, 2018, a Jetlux email account sent four credit card authorization forms authorizing Charter Company-1 to charge an Amex card issued to Celebrity-2 in the amounts of $45,000, $40,000, $40,000, and $1,100. Each authorization form bore the purported signature of Celebrity-2. Charter Company-1 processed "block" or "authorization" transactions on Celebrity-2's Amex card corresponding to the amounts on the credit card authorization forms, with the expectation that Jetlux would soon make payment in full by wire, at which point Charter Company-1would release these "block" transactions. On or about April 5, 2018, Osovitzki himself assured Charter Company-1's CEO via WhatsApp text messages that he had ordered that his bank send the wire payment, but that an error in the account number caused the bank to fail to process it. Over the next several days, Osovitzki repeatedly assured Charter Company-1's CEO that the wire had been sent. Charter Company-1's CEO requested that Osovitzki provide confirmation of the wire transfer. Osovitzki stated that he would do so, but neither the confirmation nor the wire payment ever arrived. Eventually, Osovitzki ceased responding to Charter Company-1's requests for payment. By on or about April 23, 2018, Celebrity-2 informed Amex that she had not authorized any charges to her credit card by Charter Company-1. As a result, by May 21, 2018, Charter Company-1 was forced to refund Amex for the

charges to Celebrity-2's Amex Card. By letter dated September 25, 2018, Celebrity-2 informed Amex that she had not signed Charter Company-1's credit card authorization forms, and had actually paid Jetlux for the April 2, 2018 charter flight from Shanghai to Paris in advance. Ultimately, Amex returned approximately $126,000 to Charter Company-1. However, because Celebrity-2 had not authorized the charges to Celebrity-2's Amex Card, and was deemed not responsible for the charges, Amex suffered a loss of approximately $126,000. (*E.g.*, Email Aff. ¶¶ 14(a)-(h)).

2. The Supporting Affidavits' Probable Cause to Believe That the Places or Items to be Searched Contained Evidence, Fruits and Instrumentalities of the Subject Offenses

The Supporting Affidavits also set forth probable cause to believe that the subject email accounts, the cellphone location data, the premises, and the Hummer contained evidence, fruit, and instrumentalities of the Subject Offenses under investigation.

a. The Email Affidavit

In addition to the foregoing, the Email Affidavit noted that each of the six email accounts to be searched had been "used to send or receive email communications associated with unauthorized credit card transactions to or from Amex, victims of the Force-Post Scheme, victims of the Unauthorized Credit Card Transaction Scheme, and/or charter flight companies." (Email Aff. ¶ 15). As examples, the Email Affidavit noted that:

- Subject Account-1 (tom.osovitzki@ctmstravel.com) received email correspondence from victim Amex relating to Osovitzki's Amex credit card used for many of the force-post transactions. (Email Aff. ¶¶ 11(d), 12(a)(b), (c), (i), (j), 15(a)).

- Subject Account-2 (galia.osovitzki@ctmstravel.com) received email correspondence from victim Amex relating to Osovitzki's mother's Amex credit card that was used for force-post transactions. (Email Aff. ¶¶ 11(f), 12(g), (h), (i), 15(b)).

- Subject Account-3 (tom.osovitzki@jetlux.com) exchanged emails with Subject Account-4 and charter flight company Victim-3 relating to fraudulent authorization codes and credit card transactions. (Email Aff. ¶¶ 12 (e)-(j)).

- Subject Account-4 (camila.febus@jetlux.com) exchanged emails with Subject Account-3 and charter flight company Victim-3 relating to fraudulent authorization codes and credit card transactions. (Email Aff. ¶¶ 12 (e)-(j)). Subject Account-4 was also used to

communicate with charter flight companies in connection with Jetlux's unauthorized use of its customers' credit cards. (Email Aff. ¶ 13(d), 13(e), 14, 15(e)).

- Subject Account-5 (marie.capre@jetlux.com) is known to have been used to communicate with at least one charter flight company in connection with Jetlux's unauthorized use of a customer's credit card. Further, Jetlux's agents typically booked charter flights via email, and several charter companies Jetlux paid using customers' credit cards without authorization informed that customer that Marie Capre booked the flights. (Email Aff. ¶¶ 12(e), (f), 15(e), (f)).

- Subject Account-6 (tomo@revelife.com) was the account to which Osovitzki requested a victim charter flight company send Osovitzki documentation relating to a flight for which Jetlux provided the victim charter flight company credit card authorizations bearing Celebrity-2's forged signatures. (Email Aff. ¶¶ 14).

b. The Cellphone Location Affidavit

The Cellphone Location Affidavit set forth the following facts, among others, related to the place to be searched:

- Jetlux was the subscriber of the target cellphone. Osovitzki used the target cellphone in connection with Jetlux business, and had provided the target cellphone as his mobile telephone number in emails from at least in or about 2009 through at least December 20, 2018. (Cellphone Location Aff. ¶ 23).

c. The Office Affidavit

The Office Affidavit set forth the following facts, among others, related to the place to be searched:

- Jetlux and other companies owned and operated by the Osovitzki family had operated out of an office in Aventura, Florida, until the beginning of April 2019, but had recently requested that the mail for Jetlux and the other businesses be forwarded, effective April 13, 2019, to the Office, which both Osovitzki and his father were observed entering the day before the warrant issued. (Office Aff. ¶¶ 30-35). The Office Affidavit also noted that, based on the affiant's training, experience, participation in other fraud investigations, and discussions with other law enforcement officers experienced in fraud investigations, the affiant was aware that records of financial transactions are often kept several years, and that when businesses change office locations, they typically move business records, computers, and electronic devices to the new location. (*Id.* ¶ 36).

d. The Home Affidavit

The Home Affidavit set forth the following facts, among others, related to the place to be searched:

- Osovitzki and his wife were the owners of the Home. (Home Aff. ¶ 34).

- The Home was the mailing address for Osovitzki and his wife's Amex credit cards that were utilized in the force-post scheme, and where Amex had mailed them correspondence, including correspondence relating to Amex's cancellation of those cards and transactions that occurred after the cards had been cancelled. (*Id*. ¶ 32).

- Florida Department of Motor Vehicles records reflected that the Home was the residence address of Osovitzki and his wife, but the chief financial officer of CTMS Travel Group[4] reported that while Osovitzki and his wife had lived together at the Home until their recent separation, Osovitzki was no longer residing at the Home. (*Id*. ¶ 33, 35),

- Both Osovitzki and his wife engaged in email and text communications relating to the Subject Offenses and the operations of Jetlux at times when they were likely to have been at their residence. Specifically, Osovitzki's wife participated in the operations of Jetlux, and received email correspondence from at least two of the victims of the force-post scheme; Osovitzki was frequently in email and text communication with customers late at night in connection with last minute travel requests; and both Osovitzki and his wife sent Jetlux-related email communications in the late evening and early morning (*e.g.*, between 11:00 p.m. and 2:00 a.m.). (*Id*. ¶¶ 38, 39).

- Based on the affiant agent's training, experience, participation in other fraud investigations, and discussions with other law enforcement officers experiences in fraud investigations, business owners commonly store business records at both the business's physical location and their home, particularly when both owners of the home participate in the business's operations. (*Id*. ¶ 40).

e. The Parents' Residence Affidavit

The Parents' Residence Affidavit set forth the following facts, among others, related to the place to be searched:

- The subject premises was the residence of Osovitzki's parents, an apartment inside a high-rise apartment/condominium building, and the mailing address for two of Osovitzki's

[4] The Home, Parents' Residence, and Apartment Affidavits noted that Osovitzki's parents founded and operated CTMS Travel Group ("CTMS"), a Canadian company that provided corporate travel management services, including aircraft charter flight services. (*E.g.* Home Affidavit ¶ 18).

mother's credit cards that were utilized for transactions that were part of the force-post scheme. (Parents' Residence Aff. ¶¶ 8(d), 8(e), 14, 18, 19, 34, 36).

- On or about April 18, 2019 (the month before the warrant issued), the affiant FBI agent had observed Osovitzki and his father as they exited the front lobby of the building together and placed an item in the trunk of a silver Hummer in which they then departed together. (*Id.* ¶ 35).

- From on or about December 30, 2018, through on or about March 1, 2019, one of Osovitzki's mother's Amex credit cards was used in connection with approximately 24 credit card transactions that were processed through the POSD for CTMS UK, Ltd ("CTMS UK"), totaling approximately $369,640. Because Amex had cancelled that card, and had not provided those authorization codes, it ultimately declined all 24 CTMS UK transactions. However, because authorization codes had been entered into the POSD in connection with the transactions, they were processed by one of Amex's payment processors, and some portion of the funds were paid into a CTMS UK merchant account linked to a Barclay's bank account held by CTMS UK. The same Amex credit card of Osovitzki's mother was used, on or about March 3, 2019, in connection with a $20,000 transaction processed through a POSD for an entity named Onyx Air, LLC DBA Titan Aviation ("Titan"). At Amex's request, Titan's Charter Sales Manager, using the name "Marie Capre," sent Amex records relating to the transaction, including a purported payment authorization form bearing the purported signature of Osovitzki's mother and the credit card information for Osovitzki's mother's Amex credit card. The authorization purported to authorize Titan to charge $20,000 to the card as a deposit for a $57,100 March 3, 2019 charter flight. Like the earlier CTMS UK transactions above, Amex ultimately declined this charge. The Parents' Residence Affidavit noted that the Titan Aviation invoice for the flight indicated that the flight was arranged for an entity with a listed address of the Parents' Residence. In addition, some of Osovitzki's tom.osovitzki@jetlux.com emails stated that Jetlux was "a CTMS Travel Group Company," Osovitzki also used the email address tom.osovitzki@ctmstravel.com, and Osovitzki's mother was actively involved in the operation of CTMS. (*Id.* ¶¶ 17, 19, 37).

- Capre reported to the agent affiant that she had worked at Jetlux, reporting directly to Osovitzki, and that after charter companies complained about Jetlux's practices, including those related to the fraudulent authorization codes, Osovitzki falsely informed some that he had fired Capre for stealing from Jetlux, as part of his explanation as to why Jetlux was not able to pay the charter companies what they were owed. Capre reported, however, that Osovitzki had not in fact fired her, but instead had her adopt the use of an alias, and corresponding email address, camila.febus@jetlux.com so that she could continue to work with charter companies that believed Capre was no longer working at Jetlux. Text messages provided by Capre reflected that she had exchanged text messages with Osovitzki's mother relating to the operations of Jetlux, including a May 24, 2018 text message in which Capre sent Osovitzki's mother contact information for the chief operating officer of a victim charter flight company, with the additional information that he was a "[v]ery nice guy. Super respectful do not mention MARIE he thinks I quit," followed by "Camila," and "Only Camila." (*Id.* ¶¶ 20, 21, 38).

- Based on the agent affiant's training, experience, participation in other fraud investigations, and discussions with other law enforcement officers experienced in fraud investigations, business owners commonly store business records at both the business's physical location and their home, and that records of financial transactions in particular are often kept several years, including those "deleted" from electronic devices. (*Id.* ¶ 39).

f. The Apartment Residence Affidavit

The Apartment Residence Affidavit set forth the following facts, among others, related to the place to be searched:

- CTMS's chief operating officer had reported that Osovitzki had recently moved from the home he shared with his wife, following their recent separation. On or about March 1, 2019, Osovitzki began leasing the Apartment Residence, an apartment in a condominium/apartment complex, in the name of Osovitzki and one of his companies, Revelife. Osovitzki also utilized email address tomo@revelife.com in connection Jetlux business. The property manager for the condominium/apartment complex reported that Osovitzki had provided tom.osovitzki@jetlux.com as his contact email address, and moved into the Apartment Residence, a three-bedroom apartment, on or about March 7, 2019. Osovitzki was frequently in email and text communications with customers late at night in connection with last minute travel requests, and frequently sent Jetlux-related email communications, including from his tom.osovitzki@jetlux.com email account, in the late evening and early morning (*e.g.*, between 11:00 p.m. and 2:00 a.m.). (Apartment Residence Aff. ¶¶ 38, 39, 43).

- Based on the affiant agent's training, experience, participation in other fraud investigations, and discussions with other law enforcement officers experienced in fraud investigations, business owners commonly store business records at both the business's physical location and their home. (*Id*. ¶ 46).

g.The Hummer Affidavit

The Hummer Affidavit set forth the following facts, among others, related to the place to be searched:

- The Hummer was registered to Osovitzki, and was observed to be parked at Osovitzki's new office two days before the warrant was sought. (Hummer Aff. ¶¶ 32, 33-37).

- The day before the warrant was sought, law enforcement officers searched and seized from Osovitzki's new office materials relating to the operation of Jetlux, including credit cards in the name of Osovitzki's wife and mother (*Id*. ¶ 37).

- The day before the warrant was sought, agents located the Hummer in the parking garage of Osovitzki's new Apartment Residence, and an FBI agent looking through the Hummer's

windows observed it to contain what appeared to be a passport and mail matter, including a federal express envelope and mail from the Florida Department of Transportation. (*Id.* ¶¶ 33, 38).

- The day before the warrant was sought, Osovitzki reported to agents that his phone might be in his car. Law enforcement officers located a cell phone within Osovitzki's new Apartment Residence, but also located more than a dozen other cell phones that very same day at Osovitzki's new office at a time when it was not yet occupied. (*Id.* ¶ 40).

h. The Premises and Hummer Affidavits' Additional Probable Cause Concerning Electronically Stored Information

In addition to the foregoing concerning Osovitzki and Jetlux's use of electronic devices for telephone calls, email, text messaging, WhatsApp messaging, and document delivery, each of the Premises Affidavits and the Hummer Affidavit set forth additional information specifically supporting the search of electronically stored information ("ESI"), including the following:

- Based on the agent affiant's training and experience, individuals who engage in wire fraud involving email communications in connection with their operation of a business commonly use computers and other electronic devices to access their email accounts and generate and store business records. (*E.g.*, Office Aff. ¶ 37).

- Where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred, because, among other things, electronic files can be stored on a hard drive for years at little or no cost, and even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. (*E.g.*, *Id.* ¶ 38).

3. The Supporting Affidavits' Requests for Particularized Material

The Supporting Affidavits requested that the court issue warrants allowing for the search of the Email Accounts, Premises, and Hummer for specified evidence, fruits, and instrumentalities of the Subject Offenses.

a. The Email Affidavit

The Email Affidavit requested that the court issue a warrant requiring Microsoft to produce, for each of the six email accounts, email content, address book information, subscriber and payment information, transactional records, customer correspondence, and preserved or

backup records, and authorizing law enforcement personnel to search that material for "evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud) and 1349 (conspiracy to commit wire fraud)." (Email Affidavit Attachment A). The Email Affidavit further focused that request by listing the following specific, enumerated categories of the types of information that would come within the scope of the Email Warrant: (i) Evidence of the Subject Offenses, those violations occurring on or after March 1, 2017, including correspondence relating to declined credit card transactions, "force-post" credit card transactions, authorization codes, or unauthorized credit card transactions, including but not limited to transactions involving the Amex accounts of Osovitzki, his mother, his wife, and certain victims identified by account number in both the Email Affidavit and the Email Warrant's Attachment A; correspondence with Amex, certain victims identified by name in both the Email Affidavit and the Email Warrant's Attachment A, and other victims and potential victims; and correspondence containing fraudulent representations in furtherance of the Subject Offenses; (ii) Evidence of the identities and/or location of the user(s) of the Subject Accounts, co-conspirators, and/or additional victims, including correspondence with co-conspirators relating to the commission of the Subject Offenses; (iii) Evidence concerning the location of other evidence, including additional email accounts or credit card accounts used in furtherance of the Subject Offenses; and (iv) Passwords and other information needed to access computers or other accounts used in furtherance of the Subject Offenses. (Email Aff. ¶¶ 16-17, Email Warrant Attachment A, Part III).

b.The Cellphone Location Affidavit

The Cellphone Location Affidavit requested that the court issue a warrant requiring Verizon Wireless to produce "prospective location information" and "historical location information," for a cellphone subscribed to in the name "Jet Lux, Inc." and used by Osovitzki in

connection with the Subject Offenses. (Cellphone Location Aff. ¶ 2, 4, 22(d), 23(b); Cellphone Location Warrant ¶¶ 7, 8).

c. The Premises and Hummer Affidavits

The Premises and Hummer Affidavits requested that the court issue warrants authorizing searches for "evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), and 1028A(a)(1) (aggravated identity theft)," and further focused that request by listing specific, enumerated categories of the types of information that would come within the scope of the warrants. Those categories included (i) Documents, records and correspondence concerning declined credit card transactions, "force-post" credit card transactions, authorization codes, unauthorized credit card transactions, disputes with American Express or any other credit card company, theft from Jetlux, Inc. ("Jetlux") or theft by any Jetlux employee; (ii) Documents, records, correspondence containing or relating to fraudulent representations in furtherance of the Subject Offenses, including credit card transactions involving the use of credit cards belonging to others, or the use of authorization codes purportedly provided by American Express or any other credit card company; (iii) Documents, records and correspondence concerning the management structure or reflecting the exercise of management authority of Jetlux, CTMS Travel Group, or CTMS UK, Ltd., or any other companies in the business of brokering air travel operated by Tomer Osovitzki; (iv) Communications between Tomer Osovitzki and any accomplices, confederates or aiders and abettors in the Subject Offenses, or any employees of Jetlux, CTMS Travel Group, or CTMS UK, Ltd. relating to the Subject Offenses; (v) Financial records, including books, ledgers, credit card bills, and financial instruments related to Jetlux, CTMS Travel Group, CTMS UK, Ltd., or any air travel business operated by Tomer Osovitzki; (vi) Credit card Point of Sale Devices; and (vii) Computer devices, storage media, and related

electronic equipment used to access, transmit, or store information relating to the Subject Offenses. (*E.g.* Office Aff. ¶ 46; Office Warrant, Attachment B).

As noted above, and based upon those applications, reviewing United States Magistrate Judges in this District and the Southern District of Florida authorized each application and approved the Email, Cellphone Location, Office, Home, Parents' Residence, Apartment Residence, and Hummer warrants.

B. Discussion

The defendant moves to suppress the evidence obtained pursuant to the foregoing warrants on a number of bases, each of which is meritless. First, the warrants were amply supported by probable cause and were not overbroad, as there was probable cause to believe that the defendant and Jetlux engaged in a scheme to commit wire fraud, and that evidence of that crime would be found in the email accounts, cellphone location data, premises, and Hummer. Second, in any event, the good faith exception applies, because agents relied in good faith on the search warrants issued by United States Magistrate Judges. *Third*, Osovitzki lacks standing to challenge the searches of his mother's CTMS email account and his parents' residence.

1. Applicable Law

The Warrants Clause of the Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. Amend. IV. Probable cause is a "fluid concept" turning "on the assessment of probabilities in particular factual contexts," and as such is not "readily, or even usefully, reduced to a neat set of legal rules." *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 232 (1983) (internal quotation marks omitted)). Rather, probable cause is a "flexible, common-sense standard" that requires a case-by-case analysis of the totality of the circumstances. *Texas v. Brown*, 460 U.S. 730, 742 (1983); *see also Gates*, 462 U.S. at 230. In evaluating probable cause in any given case,

a judge must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Falso*, 544 F.3d at 117 (quoting *Gates*, 462 U.S. at 238). Moreover, probable cause requires "'only [a] probability, and not a prima facie showing,"' *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993) (quoting *Gates*, 462 U.S. at 235), and it is entirely appropriate for the reviewing judge to rely upon "'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act,"' *Walczyk v. Rio*, 496 F.3d 139, 156 (2d Cir. 2007) (quoting *Gates*, 462 U.S. at 231).

Moreover, once a search warrant has issued, "the finding of an issuing judicial officer that probable cause exists" must be "accord[ed] substantial deference." *Wagner*, 989 F.2d at 72 (internal citations omitted); *see also United States v. Nichols*, 912 F.2d 598, 602 (2d Cir. 1990) (same). Provided there is a "substantial basis for finding probable cause," *Wagner*, 989 F.2d at 72 (internal citations omitted), the issuing judge's determination cannot be disturbed. Moreover, "any doubt about the existence of probable cause will be resolved against the challenge to [the issuing judicial officer's] determination." *United States v. Bellomo*, 954 F. Supp. 630, 636 (S.D.N.Y. 1997) (citing *Gates*, 462 U.S. at 237 n.10).

In addition to its probable cause requirement, the Warrant Clause contains a prohibition against "general warrants." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). "The problem [posed by a general warrant] is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings … [the Fourth Amendment addresses the problem] by requiring a 'particular description' of the things to be seized'" as well as the place to be searched. *Id.* at 480 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

To satisfy the particularity requirement, a warrant must: (i) "identify the specific offense for which the police have established probable cause"; (ii) "describe the place to be searched"; and (iii) specify the items to be seized by their relation to designated crimes." *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) (internal quotation marks omitted). "The Fourth Amendment does not require a perfect description of the data to be searched and seized." *Id.* at 100. Rather, the requirement is satisfied if the warrant, including its attachments, enables the executing officer to ascertain and identify with reasonable certainty those items that the magistrate judge has authorized him or her to seize. *See Groh v. Ramirez*, 540 U.S. 551, 557-59 (2004); *United States v. Rosa*, 626 F.3d 56, 58 (2d Cir. 2010). Additionally, "[t]he degree to which a warrant must state its terms with particularity varies inversely with the complexity of the criminal activity investigated." *United States v. Cioffi*, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009) (quoting *United States v. Regan*, 706 F. Supp. 2d 1102, 1113 (S.D.N.Y. 1989)). "The type of evidence sought is also relevant; in particular, courts have recognized that documentary evidence may be difficult to describe *ex ante* with the same particularity as a murder weapon or stolen property." *Id.*; *see also United States v. Scully*, 108 F. Supp. 3d 59, 65-66 (E.D.N.Y. 2015) ("The level of specificity required by the Fourth Amendment depends on many factors, including the nature of the crime, and where complex financial crimes are alleged, a warrant properly provides more flexibility to the searching agents.") (internal quotation marks and citation omitted).

The probable cause and particularity requirements intersect in the doctrine of overbreadth. "[A] warrant is overbroad if its 'description of the objects to be seized … is broader than can be justified by the probable cause upon which the warrant is based."' *United States v. Lustyik*, 57 F. Supp. 3d 213, 228 (S.D.N.Y. 2014) (quoting *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013)). Naturally, the broader the crime or crimes under investigation, the broader the categories

of documents and records that may properly be seized. *See, e.g.*, *United States v. Jacobson*, 4 F. Supp. 3d 515, 522 (E.D.N.Y. 2014) (breadth of warrant was justified because "the crimes under investigation were complex and concerned a long period of time, not simply one or two dates of criminal activity"); *United States v. Levy*, 2013 WL 664712, at *8 (S.D.N.Y. 2013) (broad warrant with no timeframe limitation was justified by breadth and complexity of fraud described in underlying affidavit); *United States v. Dupree*, 781 F. Supp. 2d 116, 149 (E.D.N.Y. 2011) ("The nature of the crime … may require a broad search ....").

2. Discussion

a. The Search Warrants Were Supported by Probable Cause and Were Not Overbroad

The defendant argues that the search warrants were issued without probable cause and were overbroad. As detailed above, the applications for each warrant attached detailed affidavits specifically alleging the defendant's and Jetlux's involvement in a scheme to commit wire fraud, and dealings with customers, charter flight suppliers, and victims, including through telephone, email, and text messaging, as a part and in furtherance of those offenses. These included specific communications and documents relevant to the scheme, and those communications' connections to the places and ESI to be searched. The affidavits set forth facts that established a "fair probability that contraband or evidence of a crime" would be found in the places and ESI to be searched. *Gates*, 462 U.S. at 238.

Furthermore, the search warrants were sufficiently particular and were not overbroad. The Email, Office, Parent's Residence, Apartment Residence, and Hummer Search Warrants identified, in their Attachment A or Attachment B, the specific offenses for which there was probable cause, and specified the items to be seized by authorizing the search of "evidence, fruits,

and instrumentalities" of the subject offenses,[5] and then enumerating several categories exemplifying such evidence.[6] Such lists of illustrative enumerated categories of evidence, which clearly modify and are tethered to the specific crimes being investigated, are sufficiently particularized under the Fourth Amendment and are not overbroad. *See, e.g.*, *United States v. Riley*, 906 F.2d 841, 844-45 (2d Cir. 1990); *United States v. Young*, 745 F.2d 733, 759-60 (2d Cir. 1984); *United States v. Patel*, 16 Cr. 798 (KBF), 2017 WL 3394607, at *4-*5 (S.D.N.Y. Aug. 8, 2017); *Lustyik*, 57 F. Supp. 3d at 227-28.

i. The Email Warrant

The defendant does not appear to seriously dispute that the Email Affidavit set forth probable cause to believe the defendant and Jetlux were involved in a scheme to commit wire fraud, or that evidence of that scheme would be found in the subject email accounts. Instead, the defendant argues that the Email Warrant was overbroad in that it required Microsoft's production of emails and related ESI for the period through the date the Email Warrant issued – December 20, 2018 – whereas "the latest purported communication mentioned in the affidavit refers to an email of April 27, 2018, eight months earlier than the end of the [Email Warrant's] date range." (Email Mot. at 2). The defendant also argues that, "[a]s a wide ranging exploratory search, the [Email] Warrant constituted a 'general search' prohibited by the Fourth Amendment." (Email

[5] Search warrants that have been invalidated for insufficiently particularizing the subject offenses were far less specific than the warrants here, for they failed to specify any crime at all or alluded broadly to all state or federal law. *See Galpin*, 720 F.3d at 447 (warrant authorized search of evidence of "NYS Penal Law and or Federal Statutes"); *Rosa*, 626 F.3d at 58 (warrant failed to set forth "the nature of the suspected criminal activity"); *United States v. Bianco*, 998 F.2d 1112, 1116 (2d Cir. 1993) (warrant "made no mention of any criminal statute or criminal conduct"); *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992) ("Nothing on the face of the warrant tells the searching officers for what crime the search is being undertaken.").

[6] As discussed below, the Cellphone Location Warrant directed Verizon Wireless to produce highly particularized cellphone data without any need for a search by law enforcement officers.

Mot. at 4-6). However, aside from boilerplate citations to the general requirement of particularly and the doctrine of overbreadth, and the Email Warrant's date range limitation discussed above, he does not explain how he believes the Email Warrant is overbroad. In any event, the cases relied upon by the defendant fail to support his argument, and courts routinely have upheld the search of all emails in an account, without any temporal limitation.

The Email Warrant satisfied all three particularity requirements set forth by the Second Circuit in *Ulbricht*. First, it identified the specific federal offenses for which law enforcement had established probable cause. *See Ulbricht*, 858 F.3d at 99. Second, it described the places to be searched: specified subject email accounts. Last, it specified the items to be seized by their relation to the designated crimes. *See id.* The Email Warrant limited the seizure of information to certain categories of evidence and records, including subscriber and account information, sent and received messages, draft email messages, and attachments, which were evidence, fruits, and instrumentalities of wire fraud conspiracy to commit wire fraud. *See Scully*, 108 F. Supp. 3d at 69 (generally, a warrant that authorizes a search for documents and things that constitute evidence of a particular crime is not overbroad); *see also Ulbricht*, 858 F.3d at 100 ("[t]he Fourth Amendment does not require a perfect description of the data to be searched and seized."). Thus, the warrants were sufficiently particularized under the standard set forth in *Ulbricht*, and did not authorize the "general, exploratory rummaging in a person's belongings" that the particularity requirement prohibits, *Andresen*, 427 U.S. at 480 (internal quotation marks omitted). That should end the matter.

The defendant's arguments that that Email Warrant was overbroad in that it authorized the search of the entire contents of the subject email accounts, and the seizure of emails beyond the date of the last email communication set forth in the Email Affidavit, are unavailing and find no

support in the cases cited by the defendant or in the prevailing case law. First, the lack of any specified date ranges or other temporal restrictions alone does not render a warrant insufficiently particular or overbroad, and the cases cited by the defendant do not hold otherwise. For example, in *Galpin*, the deficiency which led to suppression was that the warrant authorized officers to search generally for evidence of "NYS Penal Law and or Federal Statutes," in violation of the Fourth Amendment's particularity requirement. 720 F.3d at 447. This was a "failure to identify the specific offense for which the police have established probable cause." *Ulbricht*, 858 F.3d at 99. Here, the Email Warrant suffers no such flaw.

While cases not cited by the defendant, such as *United States v. Wey*, 256 F. Supp. 3d 355, 388 (S.D.N.Y. 2017) and *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 459-60 (S.D.N.Y. 2013), have noted that the lack of a temporal limitation may be "relevant" to the particularity analysis, no court has held that the lack of such a limitation alone renders a warrant insufficiently particular. For example, the courts in *Wey* and *Zemlyansky* merely observed that the lack of such a limitation "reinforce[d]" the conclusion that the warrants at issue already were insufficiently particular, and that the "lack of particularity [was] only compounded by the absence of any date restriction on the items to be seized." *Wey*, 256 F. Supp. 3d at 388 (quoting *Zemlyansky*, 945 F. Supp. 2d at 459-560, and *United States v. Vilar*, 2007 WL 1075041, at *23 (S.D.N.Y. Apr. 4, 2007)). Moreover, the court in *Wey* recognized that the "complexity and duration of the alleged criminal activities" in a given case may render temporal limitations "less significant." 256 F. Supp. 3d at 388 (internal quotation marks omitted). In other words, while the presence or absence of a temporal limitation may be a consideration, it is not a dispositive factor in determining whether a warrant lacks particularity.

Moreover, here, the temporal limitation through to the date of the warrant was entirely appropriate given the breadth and scope of the conduct under investigation, as outlined in the Email Affidavit, which justified seeking the entirety of the email accounts. First, courts routinely have upheld search warrants authorizing the seizure and search of entire email accounts. *See In re Warrant for xxxxxxx@gmail.com*, 33 F. Supp. 3d 386, 390 (S.D.N.Y. 2014) ("Notably, every case of which we are aware that has entertained a suppression motion relating to the search of an email account has upheld the Government's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant."). As the Second Circuit observed in *Ulbricht*, "a search warrant does not necessarily lack particularity simply because it is broad." *Id.* The Court reasoned:

> Since a search of a computer is akin to a search of a residence, searches of computers may sometimes need to be as broad as searches of residences pursuant to warrants. Similarly, traditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the object of the search to at least superficial examination in order to identify and seize those records that are. And in many cases, the volume of records properly subject to seizure because of their evidentiary value may be vast.

858 F.3d 71, 100. (internal quotation marks and citation omitted). Accordingly, "courts have long recognized the practical need for law enforcement to exercise dominion over documents not within the scope of the warrant in order to determine whether they fall within the warrant." *In re Warrant for xxxxxxx@gmail.com*, 33 F. Supp. 3d at 392. As the Supreme Court observed in *Andresen*, "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." 427 U.S. at 481 n. 11. "[A]llowing some latitude in this regard simply recognizes that few people keep documents of their criminal transactions in a folder marked 'drug records."' *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990).

Significantly, these principles have been applied by courts to digital evidence, including email accounts, as courts have "developed a more flexible approach to the execution of search warrants for electronic evidence." *United States v. Metter*, 860 F. Supp. 2d 205, 214 (E.D.N.Y. 2012). This includes the practical need "to access an entire email account in order to conduct a search for emails within the limited categories contained in the warrant." *In re Warrant for xxxxxxx@gmail.com*, 33 F. Supp. 3d at 392. Courts have acknowledged that "[s]earches for documents (whether in electronic or paper form) pose unique Fourth Amendment Concerns." *United States v. Metter*, 860 F. Supp. 2d 205, 213 (E.D.N.Y. 2012). "As technology and white collar and other complex criminal litigation evolved," courts have begun to "distinguish between the execution of search warrants seeking physical evidence such as guns and narcotics, and the execution of warrants seeking documents (whether in electronic or paper form)." *Id.* Accordingly, while it is true that there is "a heightened sensitivity to the particularity requirement in the context of digital searches," *Galpin*, 720 F.3d at 447, there is a concurrent sensitivity to the need to extend the principle highlighted in *Andresen* and *Riley* to email searches. While "remain[ing] sensitive to the difficulties associated with preserving a criminal defendant's privacy while searching through his electronic data," the "invasion of a criminal defendant's privacy is inevitable, however, in almost any warranted search because 'in searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."' *Ulbricht*, 858 F.3d at 103 (quoting *Andresen*, 427 U.S. at 482 n.11).

Accordingly, the Email Warrant did not lack particularity simply because it authorized the search of the entire subject email accounts to identify the particular evidence outlined in the warrant.

Similarly, the Email Warrant was not overbroad merely because it authorized the search and seizure of evidence throughout the entire subject email accounts. Rather, the authorization of a broad search across the subject email accounts for evidence of the crimes enumerated in the Email Warrant was supported by ample evidence contained in the Email Affidavit.

At the outset, "[t]he task of the issuing magistrate [or judge] is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Falso*, 544 F.3d at 117 (quoting *Gates*, 462 U.S. at 232). Accordingly, a reviewing court must afford "great deference" to the issuing court's probable cause determination. *Id.* (internal quotation marks omitted). "Thus, the task of a reviewing court is simply to ensure that the 'totality of the circumstances' afforded the magistrate a 'substantial basis' for making the requisite probable cause determination." *United States v. Clark*, 638 F.3d 89, 93 (2d Cir. 2011) (quoting *Gates*, 462 U.S. at 238). Probable cause, after all, requires "'only [a] probability, and not a prima facie showing."' *Wagner*, 989 F.2d at 72 (quoting *Gates*, 462 U.S. at 235).

As discussed above, the Email Affidavit set forth detailed information about Osovitzki's and Jetlux's involvement in repeated fraudulent Amex credit card transactions over a period of more than a year, totaling more than $2 million, and involving numerous victim charter flight companies and other victim merchants, and at least six different Amex accounts of Osovitzki, two of his family members, and three Jetlux customers. It further set forth the connection of each of the subject email accounts to those transactions based upon email communications between those email accounts and Amex, identified victim customers, and charter flight companies. Accordingly, the Email Warrant's description of the information to be seized—emails evidencing the crimes of wire fraud and conspiracy to commit same—was fully supported by the substantial probable cause

upon which it was based. *See Lustyik*, 57 F. Supp. 3d at 223; *Zemlyanksy*, 945 F. Supp. 2d at 464 ("In determining whether a warrant is overbroad, courts must focus on 'whether there exists probable cause to support the breadth of the search that was authorized."') (quoting *United States v. Hernandez*, 2010 WL 26544, *8 (S.D.N.Y. 2010)). The proper breadth of a warrant depends on the nature of the crime, and in this case the facts outlined in the warrant affidavits justified a broad search of the target email accounts. *See Jacobson*, 4 F. Supp. 3d at 522 (breadth of warrant was justified given complexity of crimes and length of time covered).

In any event, in light of the number of then-identified fraudulent transactions, the lengthy time period over which they took place, and the number of credit cards and victims involved through April 2018, the reviewing judge was entitled to find that there was a "fair probability that . . . evidence of a crime," *Gates*, 462 U.S. at 238, would be found in emails sent and received through the subject accounts through the date the warrant issued, including because the accounts probably were used after April 2018 for communications relating to fraudulent transactions that took place both before and after April 2018. The reviewing judge was entitled to make a "practical, commonsense" determination based upon "all the circumstances set forth in the affidavit," *Gates*, 462 U.S. at 238, that the subject accounts continued to be used after April 2018 for (i) communications with other, not-yet-unidentified victim customers, charter flight companies, and credit card companies concerning "force-post" and other unauthorized credit card transactions; (ii) internal emails with other Jetlux-related accounts concerning force-post and other unauthorized credit card transactions both before and after April 2018; (iii) emails with identified and not-yet-identified victims, internal Jetlux-related email accounts, and/or lenders, or the lack thereof, relating to the multiple explanations Osovitzki provided for Jetlux's failure to pay its obligations to charter flight companies, including his February 2018 claim that Jetlux had "experienced

internal theft and we have had to take a loan," (Email Aff. ¶ 12(j)); and (iv) communications that would serve as evidence of the identities and/or locations of the users of the Subject Accounts. Accordingly, the defendant's Email Motion should be denied.

ii. The Cellphone Location Warrant

The defendant argues that the Cellphone Location warrant was not supported by probable cause, lacked particularity, and constituted a "general search" prohibited by the Fourth Amendment. (Def.'s Cellphone Location Mot. at 2-7). Yet the boilerplate authority the defendant cites does not support his arguments.

With respect to probable cause, the defendant's arguments focus largely on *Carpenter v. United States*, 138 S. Ct. 2206 (2018), where the Government had obtained historical cellphone location records by means of an order obtained pursuant to 18 U.S.C. § 2703(d), as opposed to a search warrant. *Carpenter* held that the third-party doctrine does not apply to retrospective collection of cellphone location information for periods of at least seven days, and that the Government's collection of such information from the defendant's cellphone service provider constituted a search requiring a warrant supported by probable cause. *Id.* at 2217. Here, of course, the Government did obtain the cellphone location data pursuant to a warrant, and the defendant provides no explanation as to how *Carpenter* or any of the other cases he cites provide any support for his argument that the Cellphone Tracking Affidavit lacked probable cause. Nor can he do so, given the substantial probable cause it contains. (*See* Cellphone Location Aff. ¶¶ 7-24).

With respect to his particularity argument, the defendant simply points out that a "warrant must identify the items to be seized and their relation to the designated crime," (Def.'s Cellphone Location Mot. at 7) (quoting *Galpin*, 720 F.3d at 444-46), and that "the particularity requirement is violated where a warrant fails to place some 'limitation . . . on the kind of evidence sought' and

instead '[l]eaves it entirely to the discretion of the officials conducting the search to decide what items [a]re to be seized." (Def.'s Cellphone Location Mot. at 7) (quoting *United States v. Buck*, 813 F.2d 588, 592 (2d Cir. 1987)). Here, however, far from leaving the decision regarding what items would be seized to the discretion of law enforcement officers, the Cellphone Location Warrant did not leave *any* discretion to law enforcement; rather, it required Verizon Wireless to provide specific records to the FBI, principally including the Target Cellphone's historical location information, from March 1, 2017, to the date of the warrant and order, and prospective location information, for a period of 45 days from the issuance of the warrant and order. Thus, there can be no question that the warrant described the items to be produced with great particularity, and the defendant provides neither argument nor legal authority to the contrary.

With respect to overbreadth, the defendant merely states that an "otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based." (Cellphone Location Motion at 7) (quoting *Ulbricht*, 858 F.3d at 100). Again, the defendant does not address the substantial probable cause set forth in the Cellphone Location Warrant, including, among other things, Osovitzki's apparent personal involvement in many of the fraudulent transactions, which took place from March 2017 through at least April 2018, and his use of the Target Cellphone, subscribed to in the name of Jetlux, in connection with Jetlux business. Osovitzki's cellphone's locations (*i.e.* Osovitzki's own likely locations) over time could be expected to provide evidence showing, among other things, how frequently and during what time periods he was present at the Jetlux office while the fraud was underway. Moreover, the prospective location information could be expected to provide evidence of the location of the cellphone and its contents, which the Cellphone Location Affidavit set forth probable cause to believe were themselves instrumentalities and

evidence of the Subject Offenses. (*See, e.g.*, Cellphone Location Aff. ¶ 22(b)). Accordingly, the defendant's Cellphone Location Motion should be denied.[7]

iii. The Premises and Hummer Warrants

Again, the defendant does not seriously dispute that the Premises and Hummer Affidavits set forth probable cause to believe the defendant and Jetlux were involved in a scheme to commit wire fraud. Rather, the defendant appears to argue only that the affidavits failed to set forth probable cause to believe that evidence of the Subject Offenses would be found in the four premises and the Hummer. That argument clearly fails.

First, there was probable cause to believe that evidence would be found at the Jetlux Office (Premises-1). Indeed, Jetlux is the very company through which Osovitzki was perpetrating the fraud. (*See* Office Aff. ¶¶ 5-29).

Second, there was probable cause to believe that evidence would be found at the Home of Osovitzki and his wife (Premises-2). The Home was the mailing address for the Amex credit cards of Osovitzki and his wife that were utilized in the force-post scheme. (Home Aff. ¶ 32). Amex had mailed correspondence, including correspondence relating to Amex's cancellation of those cards and post-cancellation transactions to the Home. (*Id.*). Osovitzki's wife participated in the operations of Jetlux. (*Id.* ¶ 38(b)-(d)). And both Osovitzki and his wife engaged in email and text communications relating to the Subject Offenses and the operations of Jetlux at times when they

[7] The Government further notes that Pen Register and toll records information do not require a warrant issued upon probable cause. (*See* Cellphone Location Application ¶ 5 & n.3).

were likely to have been at their residence, in that they sent Jetlux-related email communications in the late evening and early morning (*e.g.*, between 11:00 p.m. and 2:00 a.m.). (*Id.* ¶ 38(a)).

Third, there was probable cause to believe that evidence would be found at Osovitzki's Parents' Residence (Premises-3). The Parents' Residence was the mailing address for two of Osovitzki's mother's credit cards that were utilized for transactions that were part of the force-post scheme. (Parents' Residence Aff. ¶ 36). Osovitzki represented that Jetlux was "a CTMS travel group company." (*Id.* ¶ 17). Osovitzki's parents operated CTMS. (*Id.* ¶ 15). Several of Jetlux's customer's also did business with CTMS. (*Id.* ¶ 16). Osovitzki's mother exchanged text messages with Capre concerning the operations of Jetlux. (*Id.* ¶ 38). And further evidence pointed to Osovitzki's mother's involvement. From on or about December 30, 2018, through on or about March 1, 2019, one of Osovitzki's mother's cancelled Amex credit cards was used in connection with approximately 24 "force post" transactions with fraudulent authorization codes, processed through a POSD for CTMS UK and totaling approximately $369,640. (*Id.* ¶ 18(a)). The same cancelled Amex credit card of Osovitzki's mother was used, on or about March 3, 2019, in connection with a fraudulent $20,000 transaction processed through a POSD for Titan Aviation, with an invoice for a flight for a company with the address of the Parent's Residence. (*Id* ¶ 19). Finally, Capre sent a text message to Osovitzki's mother in May 2018, indicating that in dealing with the operator of one of the victim charter flight companies, Osovitzki's mother should refer to Capre only by her alias, "Camila." (*Id.* ¶¶ 20, 21).

Fourth, there was probable cause to believe that evidence would be found at Osovitzki's Apartment Residence (Premises-4). Osovitzki had been residing at the Apartment Residence since on or about March 7, 2019, and probably engaged in Jetlux business from the Apartment Residence, in that he frequently engaged in email and text communications with Jetlux customers

late at night in connection with last minute travel requests, and frequently sent Jetlux-related email communications in the late evening and early morning (*e.g.*, between 11:00 p.m. and 2:00 a.m.). (Apartment Residence Aff. ¶¶ 38-43). Further, Osovitzki's phone connected to a cell tower near Premises-4 daily, and every night, for more than the month prior to the issuance of the Apartment Residence Warrant. (*Id*. ¶ 45).

Fifth, there was probable cause to believe that evidence would be found in Osovitzki's Hummer. The Hummer was registered to Osovitzki and was observed, two days before the Hummer Warrant was sought, to be parked at Osovitzki's new office. (Hummer Aff. ¶¶ 32, 36). From that new office, the day before the Hummer Warrant was sought, law enforcement officers seized materials relating to the operation of Jetlux, including credit cards in the name of Osovitzki's wife and mother. (*Id*. ¶ 37). In addition, the day before the Hummer Warrant was sought, agents located the Hummer in the parking garage of Osovitzki's new Apartment Residence. (*Id*. ¶ 38). An FBI agent looking through the Hummer's windows observed it to contain what appeared to be a passport and mail matter, including a federal express envelope and mail from the Florida Department of Transportation. (*Id.*). Finally, the day before the Hummer Warrant was sought, Osovitzki reported to agents that his phone might be in his car. (*Id*. ¶ 40).

The above affidavits also set forth probable cause to believe that electronic devices such as cell phones and computers located within the Premises and Hummer would contain evidence of the Subject Offenses in the form of ESI. Indeed, the affidavits specifically identified emails and, in some cases, text messages relevant to the Subject Offenses. The existence of numerous electronic communications in furtherance of the charged schemes certainly supports the "practical, commonsense decision" that phones and other electronic devices could contain evidence of those crimes. *See, e.g.*, *Gates*, 462 U.S. at 238; *United States v. Travisano*, 724 F.2d 341, 345 (2d Cir.

1983) (issuing judge need only find "probable cause to believe that evidence of such crime is located [in the place to be searched]."); *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004) (noting that the nexus between the items sought and the particular place to be searched "may be based on 'reasonable inference' from the facts presented based on both common sense and experience.") (internal citations and quotation marks omitted). Indeed, issuing judges routinely approve search warrants for cell phones based on far less direct evidence tying the phone in question to the subject offenses. *See, e.g.*, *United States v. Romain*, No. 13 Cr. 724 (RWS), 2014 WL 6765831, at *4 (S.D.N.Y. Dec. 1, 2014) (warrant for search of cell phones seized in drug trafficking conspiracy supported by probable cause even though application did not tie particular cell phone number to the offense); *United States v. Barret*, 824 F. Supp. 2d 419, 448-49 (E.D.N.Y. 2011) (warrant for search of cell phone affirmed with no direct tie to the phone because warrant relied on recitation of events leading to defendant's arrest and agent's training and experience). The search warrants here specifically called for the seizure of such electronic devices, while limiting the search to evidence of specific crimes and providing an exemplary list of evidence that would fall within the scope of the respective search warrants.

Finally, the defendant appears to complain that the affidavits include certain general, common-sense information. (*E.g.*, Office Mot. at 4) ("Here, the agent asserts commonplace information as probable cause that evidence of a crime will be found at Premises-1."). Needless to say, however, the fact that common sense supports a conclusion (*i.e.*, probable cause that evidence would be found) does not in any way undermine the conclusion. After all, the question of probable cause is "a practical, common-sense determination." *Gates*, 462 U.S. at 238.

Accordingly, the defendant's motions claiming that the Premises and Hummer search warrants lacked probable cause and were overbroad are without merit and should be denied.

b. Law Enforcement Agents Relied on the Search Warrants in Good Faith

Even assuming that the search warrants could be deemed overbroad or unsupported by probable cause, suppression would still be improper because the executing agents relied upon them in good faith. It is well established that a deficient warrant does not "automatically dictate the suppression of all physical evidence seized." *Clark*, 638 F.3d at 99. Indeed, the Second Circuit has remarked that "suppression is 'our last resort, not our first impulse' in dealing with violations of the Fourth Amendment." *Id.* (quoting *Herring v. United States*, 555 U.S. 135, 140 (2009)). As a result, the Supreme Court has long recognized an exception to the exclusionary rule for "evidence obtained on objectively reasonable reliance on a subsequently invalidated search warrant." *United States v. Leon*, 468 U.S. 897, 922 (1984).

Here, the defendant simply asserts without explanation or support that the warrants are not subject to the good faith exception. Aside from reciting boilerplate on when good faith may not prevent suppression, however, the defense motions do not actually contend that any such circumstances are applicable to this case. That is, the defendant nowhere alleges (1) that the Supporting Affidavits contained any false information, *see Leon*, 468 U.S. at 923; (2) that the Supporting Affidavits were "so lacking in indicia of probable cause as to render reliance upon [them] unreasonable," *id.*; (3) that the warrants were "facially defective" and "omit[ted] or misstate[d] information specifically required to be contained therein, *i.e.*, 'the place to be searched, and the persons or things to be seized,' *Clark*, 638 F.3d at 102; or (4) that the issuing judges "wholly abandoned" their judicial role, *id.* at 101. Accordingly, even if this Court were to disagree with the issuing judges and find fault with the warrants in this case, there are no grounds to conclude that the agents acted in "bad faith" when executing those duly authorized warrants and,

in turn, no basis to suppress the fruits of those searches. *United States v. Tomero*, 462 F. Supp. 2d 565, 572 (S.D.N.Y. 2006).

c. The Defendant Lacks Standing To Challenge the Searches of Certain Email Accounts and His Parents' Residence

The defendant's motions to suppress should also be denied with respect to three of the six email accounts (galia.osovitzki@ctmstravel.com, camila.febus@jetlux.com, and marie.capre@jetlux.com) and his Parents' Residence, because the defendant does not have any cognizable Fourth Amendment interest in those email accounts or his Parents' Residence. The "capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place." *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). "The defendant 'bears the burden of proving . . . that he had a legitimate expectation of privacy.'" *United States v. Watson*, 404 F.3d 163, 166 (2d Cir. 2005) (quoting *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980)). To carry this burden, "a defendant must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998).

The defendant has failed to carry his burden of showing either component of a legitimate expectation of privacy in the galia.osovitzki@ctmstravel.com, camila.febus@jetlux.com, and marie.capre@jetlux.com email accounts or his Parents' Residence. The defendant asserts through counsel that the FBI "applied for and obtained a search warrant for *the Defendant's* stored electronic communications ("Email Mot. ¶ 2), but nowhere in the motion or supporting papers does the defendant claim to have a subjective expectation of privacy in these three email accounts, which apparently were used by others, or his Parents' Residence. The defendant's silence is dispositive. *See United States v. Ulbricht*, No. 14 Cr. 68 (KBF), 2014 WL 5090039, at *5 (S.D.N.Y. Oct. 10, 2014) (subjective expectation of privacy "must be established by a declaration

or other affirmative statement of the person seeking to vindicate his or her personal Fourth Amendment interest in the thing or place searched"), aff'd, 858 F.3d 71 (2d Cir. 2017).

Nor would any claim by the defendant of a subjective expectation of privacy in the galia.osovitzki@ctmstravel.com, camila.febus@jetlux.com, and marie.capre@jetlux.com email accounts or his Parents' Residence be reasonable. Courts have recognized that "[a] person has no expectation of privacy in another person's email account." *Lustyik*, 57 F. Supp. 3d at 223 (emphasis added); *see also United States v. Nazemzadeh*, No. 11 Cr. 5726, 2013 WL 544054, at *2 n.2 (S.D. Cal. Feb. 12, 2013) ("Because Defendant could have no reasonable expectation of privacy in the email accounts of others, he cannot challenge the seizure of email accounts other than his own.").

The Government is not aware of any evidence suggesting that the galia.osovitzki@ctmstravel.com, camila.febus@jetlux.com, and marie.capre@jetlux.com accounts were the defendant's, or that he had any basis for an expectation of privacy in them or his Parents' Residence, and the defendant makes no claims to the contrary. Because the defendant has "failed to prove that he had the 'legitimate expectation of privacy' to challenge the search[es]" of those email accounts, or of his Parents' Residence, the Court "need not reach the substance of his suppression motion[s]" with respect to them. *Watson*, 404 F.3d at 167.

IV. THE DEFENDANT'S MOTION FOR RELIEF FROM PREJUDICIAL JOINDER OF CHARGES SHOULD BE DENIED

The defendant asks the Court to sever the three charges against him, and grant him three separate trials. For the reasons that follow, the defendant's request should be denied.

A. Applicable Law

Rule 8(a) of the Federal Rules of Criminal Procedure permits the joinder for trial of offenses that "(1) are of the same or similar character, or (2) are based on the same act or

transaction, or (3) are connected with or constitute parts of a common scheme or plan." Fed. R. Crim. P. 8(a). The Second Circuit has "interpreted Rule 8(a) as providing a liberal standard for joinder of offenses." *United States v. Wilson*, 512 F. App'x 75, 76–77 (2d Cir. 2013) (citing *United States v. Turoff*, 853 F.2d 1037, 1042 (2d Cir.1988)). Thus, properly joined "[s]imilar charges include those that are somewhat alike, or those having a general likeness to each other." *United States v. Rivera*, 546 F.3d 245, 253 (2d Cir. 2008) (internal quotation marks omitted). Joinder is also "proper where the same evidence may be used to prove each count, or if the counts have a sufficient logical connection." *United States v. Page*, 657 F.3d 126, 129 (2d Cir. 2011) (citation and internal quotation marks omitted).

Pursuant to Rule 14 of the Federal Rules of Criminal Procedure, "[e]ven if offenses are properly joined, in certain circumstances severance may be warranted." *Page*, 657 F.3d at 129. Specifically, where joinder of offenses for trial "appears to prejudice a defendant or the government, the court may order separate trials of counts, . . . or provide any other relief that justice requires." Fed. R. Crim. P. 14(a). Yet, as the U.S. Supreme Court has explained, the rules governing joinder "are designed to promote economy and efficiency and to avoid a multiplicity of trials, so long as these objectives can be achieved without substantial prejudice to the right of the defendant[ ] to a fair trial." *Zafiro v. United States*, 506 U.S. 534, 540 (1993) (internal quotation marks omitted). A defendant seeking severance under Rule 14 must therefore carry the "heavy burden of showing joinder will result in substantial prejudice." *United States v. Amato*, 15 F.3d 230, 237 (2d Cir. 1994) (internal quotation marks omitted). "It is not enough . . . for a defendant to demonstrate that separate trials would have increased the chances of the defendant's acquittal. Instead, the defendant must show prejudice so severe as to amount to a denial of a constitutionally fair trial, or so severe that his conviction constituted a miscarriage of

justice." *United States v. Delgado*, 972 F.3d 63, 77 (2d Cir. 2020), *as amended* (Sept. 1, 2020) (internal quotation marks and alterations omitted). "The decision to grant or deny severance is committed to the sound discretion of the trial judge." *United States v. Spinelli*, 352 F.3d 48, 54 (2d Cir. 2003) (internal quotation marks omitted).

B. Discussion

The counts in the Indictment are properly joined under Rule 8, and the defendant has not met his "heavy burden" to establish that their joinder at trial exposes him to "substantial prejudice." *Amato*, 15 F.3d at 237. Turning first to propriety of joinder, the offenses in the Indictment satisfy Rule 8(a) because, among other things, they are "connected with or constitute parts of a common scheme or plan," to wit, the defendant's scheme to defraud various businesses and clients through unauthorized credit card transactions. Fed. R. Crim. P. 8(a). Count One charges conspiracy to commit wire fraud in connection with this scheme (*see* Indictment ¶¶ 1-14); Count Two charges wire fraud in connection with this scheme (*id.* ¶¶ 15-16); and Count Three charges aggravated identity theft in connection with this scheme, specifically through the unauthorized use of a victim's name, forged signature, and credit card (*id.* ¶ 17). There can be no serious argument that agreeing to commit an offense (Count One) and actually *committing* that same offense (Count Two) lack the connection required by Rule 8's liberal standards. And Count Three is no different: in the course of conspiring and committing this very same credit card fraud, the defendant committed aggravated identity theft. Were there any doubt, the Indictment's own language describing Count Two and Count Three makes plain that they are a part of the same fraudulent scheme set out in Count One. Count Two alleges wire fraud, specifically, the use of wires "in furtherance of the scheme to defraud described in Count One," and Count Three alleges

aggravated identity theft "of a particular victim in connection with the defendant's involvement in a conspiracy to commit wire fraud, as charged in Count One." (*Id.* ¶¶ 16-17).

The defendant's arguments in favor of severance are meritless. First, citing Rule 14, the defendant asserts without elaboration that the "three counts stem from separate and distinct criminal episodes" that are not "sufficiently inextricably intertwined." (Dkt. 55, at 3). As an initial matter, such a claim is likely governed not by Rule 14, but by Rule 8, which the defendant does not rely on in his motion; and, in any event, there is no requirement in the Federal Rules of Criminal Procedure or in case law that counts joined for trial be "inextricably intertwined." (*Id.*). More to the point, the defendant's bald assertion is simply an inaccurate description of the case. As explained above, the Counts all relate to a single fraud scheme. Second, the defendant asserts, "if the jury finds that guilt is proven beyond a reasonable doubt on one count, they will infer that the Defendant is guilty on every count thereby increasing the possible penalties which may be imposed." (*Id.*). Even if that were the case, it is well established that an increased likelihood of acquittals is not a basis for ordering separate trials for properly joined counts. *See, e.g.*, *Delgado*, 972 F.3d at 77.

Accordingly, the defendant's severance motion should be denied.

V. THE DEFENDANT'S MOTION TO EXCLUDE EVIDENCE OF OFFER OR SETTLEMENT PURSUANT TO RULE 408 SHOULD BE DENIED

The defendant seeks to exclude certain evidence pursuant to Rule 408 of the Federal Rules of Evidence. (Dkt. No. 60). The defendant's motion should be denied for several reasons. As an initial matter, the broad category of communications that the defendant references in his motion are voluminous; the defendant's fraud often entailed stringing along victims of the scheme with promises of payment. While it may "often [be] difficult to determine whether an offer is made 'in compromising or attempting to compromise, a claim,'" *Pierce v. F.R. Tripler & Co.*, 955 F.2d 820,

827 (2d Cir. 1992), the defendant has plainly not established that all "offers" within this broad category of communications qualify as "offers of compromise" within the meaning of Rule 408. Even some of the specific examples cited by the defendant clearly do not fall under Rule 408. Take, for example, the defendant's text messages with the CEO of Aircraft Charter Company-15. (Dkt. No. 60, at 2). Those messages show that, in fact, there is no dispute between the defendant and the CEO as to whether the defendant owed payment to the CEO for an early April 2018 deal. Instead, the messages chronicle the defendant obfuscating and misleading the CEO, in messages spanning from April through mid-June of 2018, about the defendant's attempts to make payment—about how those attempts somehow keep going awry, and how various money transfers mysteriously keep going missing. Those messages are not offers of compromise under Rule 408. *See, e.g.*, *MCI Communications Services, Inc. v. Hagan*, 641 F.3d 112, 116–17 (5th Cir. 2011) (evidence improperly excluded when "there was not yet an actual dispute or a difference of opinion about who caused the damage . . . and how much the damage [cost]"); *Big O Tire Dealers, Inc. v. Goodyear Tire & Rubber Co.*, 561 F.2d 1365, 1372–73 (10th Cir. 1977) (correspondence between parties prior to the filing of an action held "business communications" rather than "offers to compromise" and thus outside scope of Rule 408). Indeed, to the extent that what the defendant claims to be settlement offers in fact constitute "fraudulent statements," then "Rule 408 is inapplicable." Fed. R. Evid. 408 Advisory Committee Note, 2006 Amendment.

Even if they *were* settlement offers, moreover, the Government could still properly introduce those communications for "another purpose" not prohibited by Rule 408. Fed. R. Evid. 408(b). Indeed, trial courts have "broad discretion in determining whether a statement is admissible for 'another purpose' under Rule 408(b)," and the Second Circuit has "emphasized that Rule 408's exception intends to exempt from the absolute prohibition of the Rule evidence focused

on issues different from the elements of the primary claim in dispute in the settlement negotiations." *United States v. Wahl*, 563 F. App'x 45, 51 (2d Cir. 2014) (citation and internal quotation marks omitted). Here, those other purposes and issues could include knowledge, notice, and intent. *See, e.g.*, *id.* (noting such evidence can be used to "prove a defendant's knowledge" and citing *United States v. Gilbert*, 668 F.2d 94, 97 (2d Cir. 1981)); *Zurich Am. Ins. Co. v. Watts Indus., Inc.*, 417 F.3d 682, 689 (7th Cir. 2005) (noting such evidence can be admitted "to show knowledge and intent"); *Athey v. Farmers Ins. Exchange*, 234 F.3d 357 (8th Cir. 2000) (evidence of settlement offer by insurer was properly admitted to prove insurer's bad faith); *In re: Gen. Motors LLC Ignition Switch Litig.*, No. 14-MD-2543 (JMF), 2015 WL 7769524, at *1 –2 (S.D.N.Y. Nov. 30, 2015) (consent decree admissible to show knowledge and efforts to conceal).

Accordingly, the defendant's motion should be denied. To the extent the Government develops an intention to introduce evidence of an offer of compromise, the Government plans to confer with the defense and if necessary brief that evidence's admissibility *in limine*.

VI. THE DEFENDANT'S MOTIONS FOR DISCLOSURE AND PRESERVATION ORDERS SHOULD BE DENIED

Finally, the defendant has filed several other boilerplate motions or requests.[8] The Government addresses these miscellaneous filings particularly below.

A. Motion for Disclosure of any and all Co-Conspirator Statements the Prosecution Intends to Introduce at Trial

The defendant has filed a motion related to the admissibility of statements of co-conspirators. Rule 801(d)(2)(E) excludes from the definition of hearsay "statement[s] by a coconspirator of a party during the course and in furtherance of the conspiracy." Fed. R. Evid.

[8] The defendant has also submitted two "notices" to the Government regarding privileges, which the Government respectfully submits do not require any ruling from the Court. (Dkts. 61 (Notice of Marital Privilege), 62 (Notice of Attorney-Client Privilege)).

801(d)(2)(E). To admit a statement under Rule 801(d)(2)(E), the district court must find only by a preponderance of the evidence "(a) that there was a conspiracy, (b) that its members included the declarant and the party against whom the statement is offered, and (c) that the statement was made during the course of and in furtherance of the conspiracy." *United States v. Coppola*, 671 F.3d 220, 246 (2d Cir. 2012). "In determining the existence and membership of the alleged conspiracy, the court must consider the circumstances surrounding the statement, as well as the contents of the alleged coconspirator's statement itself." *United States v. Gupta*, 747 F.3d 111, 123 (2d Cir. 2014).

In his motion, the defendant does not seek to exclude any particular statements, but instead requests, without citing any authority, "a list of the potential statements [of co-conspirators] the Government intends to introduce at trial as well as their source and relevance" and "a preliminary hearing or pre-trial determination" on their admissibility. That request is unfounded, and the burdens that the requested procedure would impose on the Government and the Court are wholly unnecessary. *See United States v. Correa-Osorio*, 784 F.3d 11, 23-24 (1st Cir. 2015) ("If a defendant contests the admissibility of an alleged coconspirator statement, the judge may conditionally admit the evidence and put off ruling until the close of all the evidence."). Instead, to the extent that the Court denies the defendant's request, the Government intends to follow its normal practice of producing materials under 18 U.S.C. § 3500 at a reasonable time in advance of trial, and the defense may raise any specific hearsay objections closer to trial, a date for which has not yet been set. Accordingly, the defendant's motion should be denied, without prejudice to raising more specific hearsay objections.

B. Motion To Disclose and Produce *Brady* (Exculpatory) Material

The Government has already produced discovery, including any potential *Brady* material. The Government recognizes its *Brady* obligations are continuing, and will promptly disclose any *Brady* material that comes into its possession. In addition, the Court already has entered its

standard order, pursuant to Fed. R. Crim. P. 5(f), confirming the Government's disclosure obligations under *Brady* and its progeny, and summarizing the possible consequences of violating those obligations. Accordingly, the defendant's generic *Brady* motion is moot. (Dkt. No. 66).

C. Motion for Disclosure Pursuant to Rules 404(b) and 609

The Government does not presently intend to introduce any evidence pursuant to Rules 404(b) or 609 of the Federal Rules of Evidence. Should that change, the Government will promptly provide notice to the defense. Accordingly, the defendant's motion is moot.

D. Motion for Early Production of *Jencks* Material

The Government will produce materials pursuant to 18 U.S.C. § 3500, as is its usual practice, at a reasonable time in advance of trial, and in accordance with the schedule set by the Court. The Government notes that a trial date has not yet been set. Accordingly, the defendant's motion is premature.

E. Request for Notice of Intent To Call Expert Witnesses and Discovery

The Government does not presently intend to introduce any evidence pursuant to Rules 702, 703, or 705 of the Federal Rules of Evidence. Should that change, the Government will promptly provide notice to the defense. Accordingly, the defendant's motion is moot.

F. Request for Notice by Government of Intent To Introduce Evidence Pursuant to Rule 807

The Government does not presently intend to introduce any evidence pursuant to Rule 807 of the Federal Rules of Evidence. Should that change, the Government will promptly provide notice to the defense. Accordingly, the defendant's motion is moot.

G. Motion for Preservation of Recordings and Notes

The Government will maintain, as is its usual practice, notes and recordings of the types described in the defendant's motion that are in the Government's possession. Accordingly, the defendant's motion is moot.

VII. CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court deny the defendant's motions in their entirety.

Dated: New York, New York
December 4, 2020

Respectfully submitted,

AUDREY STRAUSS
Acting United States Attorney

By: */s/ Jeffrey C. Coffman*
Jeffrey C. Coffman
(914) 993-1940
Micah F. Fergenson
Assistant United States Attorneys